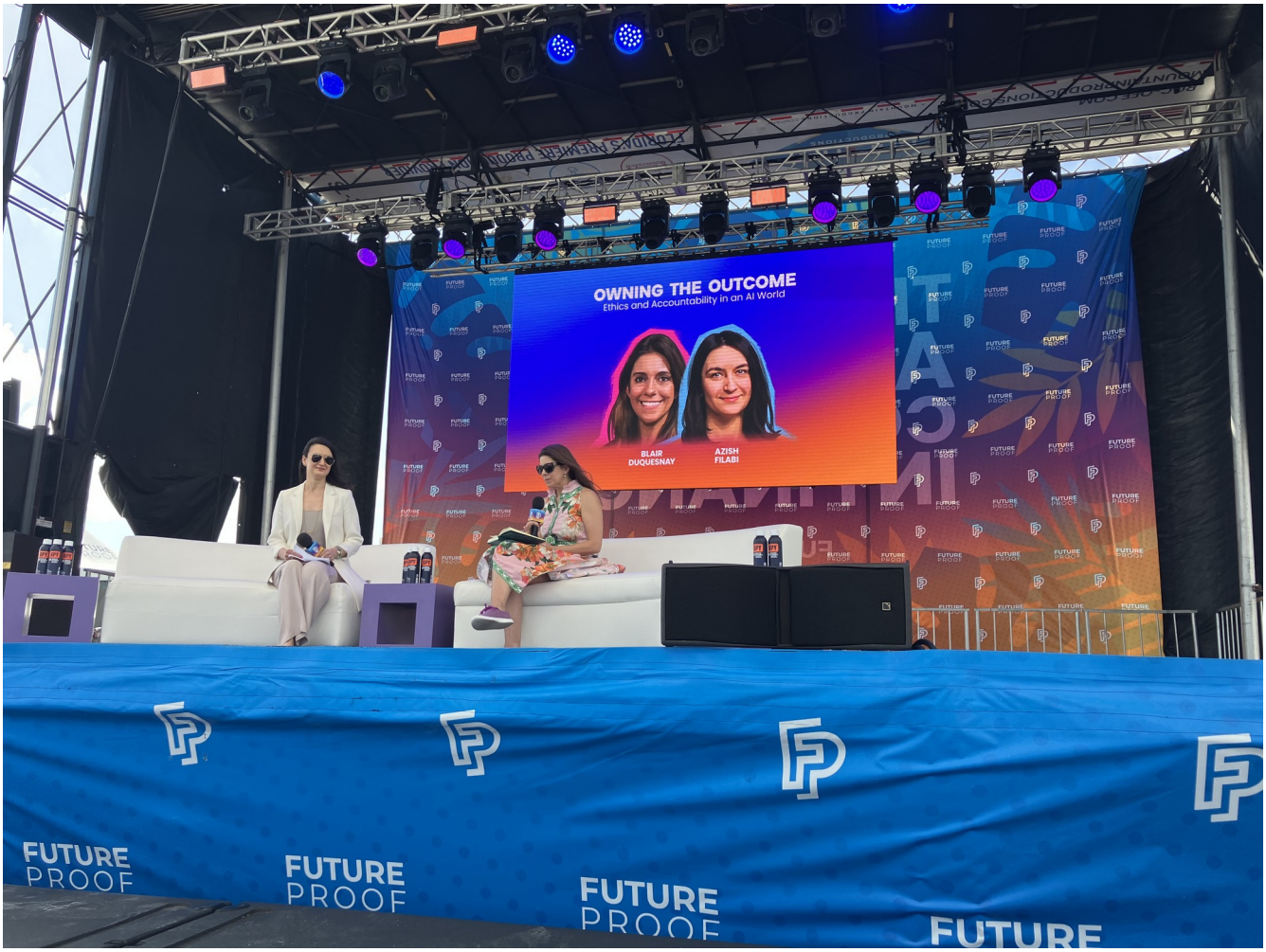
https://www.financial-planning.com/news/how-data-security-and-stress-testing-can-build-ai-trust



Blair duQuesnay, lead advisor at Ritholtz Wealth Management in New Orleans, right, interviews Azish Filabi, executive director of the Cary M. Maguire Center for Ethics in Financial Services at The American College of Financial Services, on Sunday, March 9, 2026, at Future Proof Citywide in Miami Beach, Florida.
Rob Burgess /Financial Planning

How data security and stress-testing can build AI trust
By Rob Burgess
Published March 10, 2026, 1:21 p.m. EDT

As recent research by Cerulli has shown, there is a trust gap especially between older, wealthier clients and the financial advisors who have incorporated artificial intelligence into their practices.

Being transparent with clients is certainly critical to bridging this divide, but so is a firm's ability to stress-test the infrastructure and establish clear internal guardrails for when and how AI technology will be used.

That was the focus of the "Owning the Outcome: Ethics and Accountability in an AI World" session on Sunday during the opening of the second annual Future Proof Citywide Conference in Miami Beach, Florida.

The session was moderated by Blair duQuesnay, lead advisor at Ritholtz Wealth Management in New Orleans, and featured Azish Filabi, executive director of the Cary M. Maguire Center for Ethics in Financial Services at The American College of Financial Services in King of Prussia, Pennsylvania.

duQuesnay said the competing motivations of those developing the technology and those using it are causing friction.

"Technology builders and founders move fast and break things," she said. "The financial services industry is slow and regulated and stodgy. We want to speed it up, but we need to do it the right way."

Filabi said she has observed this disconnect firsthand.

"I'll talk to the people on the computer science side and get very excited about the capabilities, and then I'll talk to firm leaders and their compliance functions are still navigating off-channel communications with text messages," she said.

Keeping the security of PII in mind

If a wealth management firm were a car, compliance would be the brake pedal, as JC Abusaid, CEO and president of Halbert Hargrove, put it at the most recent ADVISE AI conference.

As firms begin to implement AI tools into their technology stacks, now is the time to start contemplating where firms should be pumping those brakes instead of hitting the gas.

Filabi said one area where firms should slow down is how to keep clients' personally identifiable information (PII) from being used to train AI models.

Data security is of paramount importance to firms that use AI tools. But the paradox, Filabi said, is that AI systems work better when they have a lot of data. Balancing how much is acceptable to feed the AI and without introducing PII is a constant challenge, she said.

In addition, many free and even paid versions of AI chatbots don't offer the same type of privacy controls as enterprise subscriptions, making PII vulnerable to scraping.

"If you're trying to offer personalized financial products and services, and you're able to scan social media and understand life events about individuals, that's information that they put out there, but maybe not for this purpose," she said.

Despite these privacy concerns, Filabi said some clients might have an easier time sharing their finances with an automated system rather than another human, especially if there's shame involved.

"Maybe your financial portfolio looks good, but you don't have confidence in your own ability to talk about finance," she said.

Whatever balance a firm strikes, Filabi said, trust is the currency of the financial system, and any technological advancements have to preserve this.

"Having a long-term strategic perspective is vital," she said.

That's why Filabi said simple adoption is less important than the guardrails and human review firms build into their systems.

"People are more integrated into the conversation from the beginning, she said.

The rise of agentic AI increases need for stress-testing

With the rise of agentic AI, firms are now able to specify an end goal instead of feeding a chatbot a series of simple call-and-response prompts.

AI agents have already revolutionized some advisor workflows, but the convenience they provide could lead to headaches in the future without proper planning.

In the past, regulators have stipulated that they want firms to be able to audit all of their systems. However, she said, with this implementation of AI agents, she fears "that it's no longer enough." AI agents may not have undergone the rigorous testing that more established pieces of advisor tech stacks have withstood.

Filabi said she was concerned that these AI agents work well under ideal conditions, but that more challenging cases need further scrutiny by firms implementing these solutions.

She said firms should take the initiative to test their agentic AI systems more thoroughly, using less-than-ideal conditions to understand the outputs they might provide under pressure.

"It's like having a car go through a crash test in perfect conditions without a dummy in the vehicle," she said. "You're seeing that it's successful in those perfect circumstances, but you need a stress test for robustness."